Diese Kopfleiste bitte unbedingt ausfüllen!

Familienname, Vorname (bitte durch eine Leerspalte trennen)

Bereich	Berufsnummer				IHK-Nummer			Prüflingsnummer				
7	0	1	2	0	2							
Sp. 1-2		Sp. 3-6				Sp. 7-9		Sp. 10-14				

Termin: Mittwoch, 7. Mai 2025

Abschlussprüfung Sommer 2025

1202

2 Analyse und Entwicklung von Netzwerken

Fachinformatiker
Fachinformatikerin
Systemintegration

Teil 2 der Abschlussprüfung

4 Aufgaben

90 Minuten Prüfungszeit

100 Punkte

Bearbeitungshinweise

1. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, überprüfen Sie bitte die **Vollständigkeit** dieses Aufgabensatzes. Die Anzahl der zu bearbeitenden Aufgaben ist auf dem Deckblatt links angegeben. Wenden Sie sich bei Unstimmigkeiten sofort an die Aufsicht, weil Reklamationen am Ende der Prüfung nicht anerkannt werden können.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgaben** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Hilfsaufzeichnungen** können Sie das in der Tasche beigelegte Konzeptpapier verwenden. Bewertet werden jedoch grundsätzlich nur Ihre Eintragungen in diesem Aufgabensatz.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen.

1. Aufg. ☐☐ (15 16) Punkte 2. Aufg. ☐☐ (17 18) Punkte 3. Aufg. ☐☐ (19 20) Punkte 4. Aufg. ☐☐ (21 22) Punkte

Prüfungszeit ☐ (23)

Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Gesamtpunktzahl ☐☐☐ (24 25 26)

Prüfungsort, Datum

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen. Hinweis: Im Interesse einer besseren Lesbarkeit wird in der Aufgabenstellung und in den Angaben zur Aufgabenstellung nur die männliche Form (generisches Maskulinum) verwendet. Die verkürzte Sprachform beinhaltet keine Wertung und die gewählten männlichen Formulierungen gelten uneingeschränkt auch für die weiteren Geschlechter.
Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und

Korrekturrand

Die Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Sie arbeiten als Fachinformatiker (Systemintegration) bei der 1234-IT-Systemhaus GmbH. Dabei handelt es sich um einen mittelständischen IT-Dienstleister, der neben der Zentrale mehrere bundesweit verteilte Standorte hat.

Aktuell betreuen Sie für Ihren Arbeitgeber die „IHK-Wear GmbH", ein Unternehmen aus der Modebranche. Der Kunde betreibt eine Firmenzentrale in Norddeutschland und in jeder größeren Stadt mindestens eine Einzelhandels-Filiale, in der die Mode verkauft wird. Der Kunde plant aktuell einige Änderungen an der IT der Firmenzentrale sowie die Eröffnung einer neuen Filiale.

Bearbeiten Sie in diesem Zusammenhang die folgenden vier Aufgaben:
1. Aufgabe: Das bestehende Netzwerk analysieren
2. Aufgabe: Anbindung an das Internet realisieren
3. Aufgabe: Die Internetanbindung absichern
4. Aufgabe: Geräte drahtlos in das Netzwerk einbinden

1. Aufgabe (22 Punkte)

a) Das Netzwerk der IHK-Wear GmbH besteht aus der Firmenzentrale und den Filialen. Das Netzwerk in der Zentrale ist in VLANs und Subnetze aufgeteilt, wie im Netzwerkplan dargestellt.
Für alle Filialen wird der Netzbereich 172.16.200.0/22 verwendet. Die Filialen sollen nach der Modernisierung des Netzwerks Zugang zu den Servern in der Zentrale über ein VPN erhalten.

aa) Sie verschaffen sich zuerst einen Überblick über die Adressbereiche der Subnetze.

Tragen Sie die zugehörigen dezimalen Subnetzmasken sowie die Anzahl der maximal nutzbaren IP-Adressen in die Tabelle ein.
4 Punkte

VLAN ID	Name	Subnetz	Maske (dezimal)	Max. nutzbare IP-Adressen
1	default	192.168.1.0/24	255.255.255.0	254
11	Technik	192.168.11.0/26		
12	Vertrieb	192.168.12.128/25		
66	Management	192.168.66.8/29		
	Filial-Netze	172.16.200.0/22		

ab) Die Schnittstellen auf R1 werden als Gateway für die Subnetze konfiguriert. Dafür soll jeweils die letzte IP-Adresse aus dem Subnetz verwendet werden.

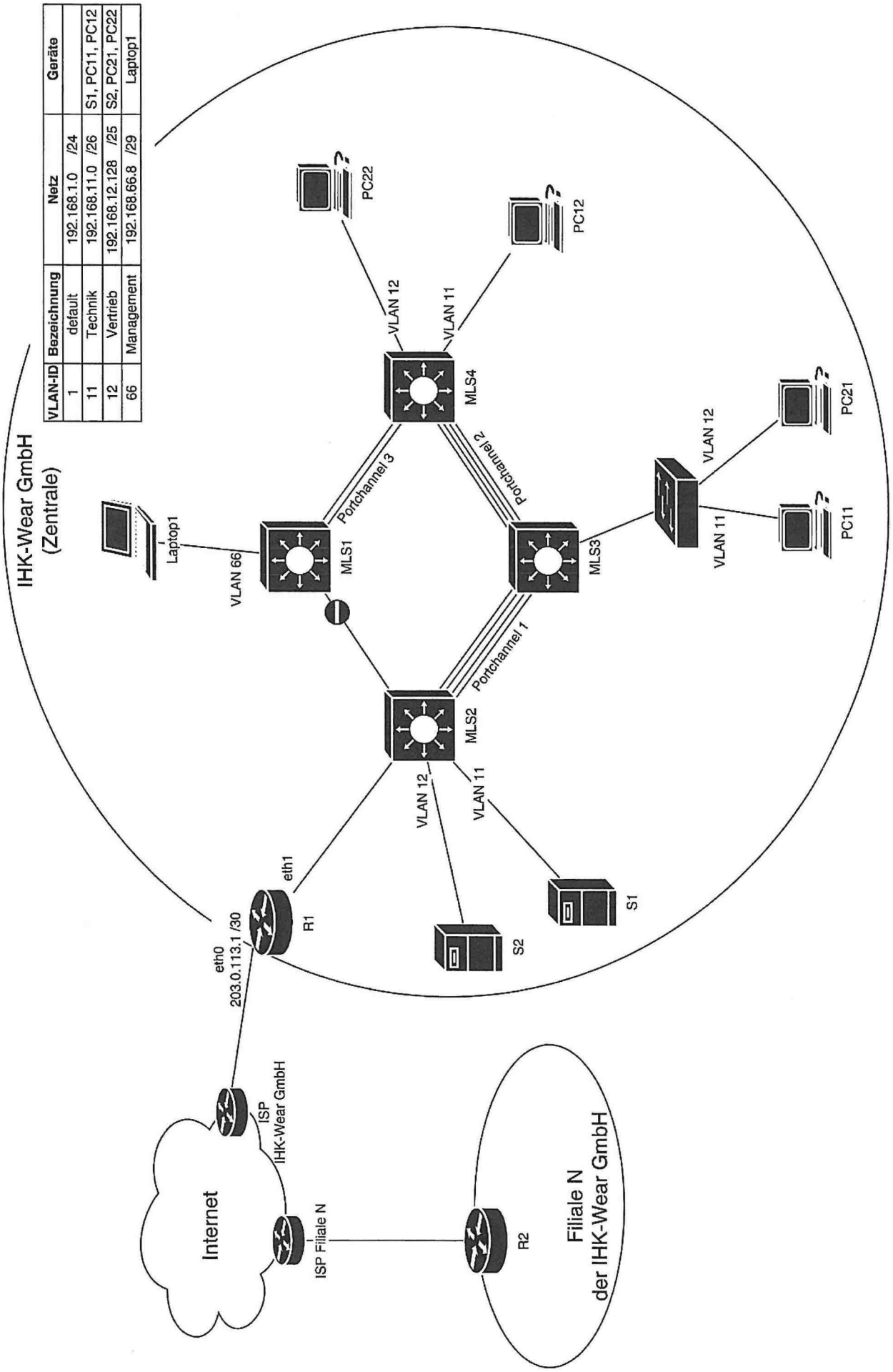
Tragen Sie die IP-Adressen der Gateways in die Tabelle ein. 4 Punkte

VLAN ID	Name	Subnetz	IP-Adresse des Gateways
1	default	192.168.1.0/24	
11	Technik	192.168.11.0/26	
12	Vertrieb	192.168.12.128/25	
66	Management	192.168.66.8/29	

Dieses Blatt kann an der Perforation aus dem Aufgabensatz herausgetrennt werden!

Anlage 1: NETZWERKSKIZZE DER IHK-WEAR GMBH

VLAN-ID	Bezeichnung	Netz	Geräte
1	default	192.168.1.0 /24	
11	Technik	192.168.11.0 /26	S1, PC11, PC12
12	Vertrieb	192.168.12.128 /25	S2, PC21, PC22
66	Management	192.168.66.8 /29	Laptop1



Korrekturrand

ac) Für die Netzwerkplanung sollen die Gateway-Adressen der Subnetze auf den Schnittstellen von R1 entsprechend der VLANs richtig zugeordnet werden.

VLAN ID	Name	Subnetz	Schnittstelle auf R1
11	Technik	192.168.11.0/26	eth1.11 (Subinterface)
12	Vertrieb	192.168.12.128/25	eth1.12 (Subinterface)
66	Management	192.168.66.8/29	eth1.66 (Subinterface)

Erläutern Sie, weshalb als Schnittstelle in der Übersichtstabelle jeweils ein Subinterface angegeben ist und was man darunter versteht. 4 Punkte

b) In der weiteren Planung wird darüber diskutiert, ob auf den Switchen „link aggregation" zum Einsatz kommen sollte.

ba) Erläutern Sie den Begriff „link aggregation" und nennen Sie zwei Vorteile gegenüber herkömmlichen Verbindungen zwischen Switchen. 4 Punkte

bb) Erläutern Sie, warum auf dem Switch MLS1 der Port mit der Verbindung zum Switch MLS2 geblockt ist (im Netzwerkplan Zeichen ⛀), obwohl er prinzipiell funktionsfähig ist. 4 Punkte

c) Nachdem der Router R1 eingerichtet wurde, können keine Verbindungen zu Adressen im Internet hergestellt werden.

Ergänzen Sie den fehlenden Eintrag in der Routingtabelle von R1, sodass Verbindungen zum Internet möglich werden. 2 Punkte

Netzwerk	Schnittstelle	Next hop
203.0.113.0/30	eth0	-
192.168.11.0/26	eth1.11	-
192.168.12.128/25	eth1.12	-
192.168.66.8/29	eth1.66	-

2. Aufgabe (29 Punkte)

Korrekturrand

a) Die IHK-Wear GmbH plant aktuell den Aufbau eines neuen Flagship-Stores in Berlin. Sie sind für die Anbindung dieser Filiale an das Firmennetz und die IT-Ausstattung der neuen Filiale zuständig.

aa) Ihr Internet-Anbieter hat Ihnen ein Angebot für die Anbindung der neuen Filiale mit einem „Geschäftskunden DSL mit 250/40 Mbit/s" vorgelegt.

Nennen Sie drei Aspekte, die einen DSL-Anschluss für Geschäftskunden von einem Privatkunden-Anschluss unterscheiden können. 3 Punkte

ab) Alternativ bietet Ihnen Ihr Internetanbieter eine „Glasfaseranbindung (GPON)" mit der gleichen Geschwindigkeit an. Ihr Anbieter weist darauf hin, dass es sich dabei um ein „shared medium" handelt.

Erläutern Sie, was man darunter versteht und warum dies für die Filiale der IHK-Wear GmbH ungünstig ist. 3 Punkte

ac) Der geplante Eröffnungszeitpunkt der Filiale liegt vor dem Termin, den Ihr Anbieter für die beiden Anschlussarten realisieren kann. Zur Überbrückung bietet Ihnen der Anbieter einen „LTE-Router mit 50/10 Mbit/s" an.

Erläutern Sie zwei Aspekte, warum dies für die Filiale keine dauerhafte Lösung ist. 4 Punkte

b) Sie haben sich für das Angebot aus Aufgabe aa („Geschäftskunden DSL mit 250/40 Mbit/s") entschieden.

ba) Nach der Bereitstellung des Anschlusses müssen Sie diesen in Betrieb nehmen. Sie erhalten für den Anschluss von Ihrem Anbieter eine öffentliche, feste IPv4-Adresse.

Erläutern Sie, wie Sie dennoch in der Lage sind, die vielen Geräte in der Filiale über diese eine IP-Adresse mit dem Internet zu verbinden. 4 Punkte

bb) Zusätzlich erhalten Sie von Ihrem Anbieter ein öffentliches IPv6-Präfix: Korrekturrand

2001:db8:9876:: /56

Sie wollen dieses Präfix für verschiedene Zwecke nutzen, daher teilen Sie diesen in Subnetze der Größe /64 auf.

Ermitteln Sie, wie viele Subnetze entstehen und wie das erste, das zweite, das vorletzte und das letzte Subnetz lautet.

5 Punkte

Anzahl Subnetze	
1. Subnetz	
2. Subnetz	
vorletztes Subnetz	
letztes Subnetz	

bc) Sie wollen in der Filiale eines der Subnetze für Server verwenden, die in einer DMZ untergebracht werden sollen.

Nennen Sie zwei Eigenschaften einer DMZ. 2 Punkte

bd) Geben Sie an, wie viele IP-Adressen in einer DMZ der Größe /64-Subnetz zur Verfügung stehen. 2 Punkte

c) Um Ihren Clients den Zugriff auf das Internet zu ermöglichen, konfigurieren Sie den Router der Filiale so, dass er für die Filiale als DNS-Server dient. Sie testen von einem Client aus die Erreichbarkeit der Seite www.ihk.de.

ca) Beschreiben Sie, wie Ihr Client die Anfrage nach www.ihk.de rekursiv aufgelöst hat. 1 Punkt

cb) Ihr Router löst die Anfrage nach www.ihk.de iterativ auf.

Erläutern Sie die einzelnen Schritte, die er dazu durchführt. 3 Punkte

Fortsetzung 2. Aufgabe →

Korrekturrand

cc) Erläutern Sie, weshalb Sie Ihren Clients in der Filiale nicht gestatten sollten, einen öffentlichen DNS-Server, wie z. B. 9.9.9.9, für die Namensauflösung zu verwenden. 2 Punkte

3. Aufgabe (29 Punkte)

Der Internetzugang der Mitarbeiter in der neuen Filiale der IHK-Wear GmbH soll unter anderem durch eine sogenannte Stateful Packet Inspection Firewall (SPI) abgesichert werden.

a) Sie unterstützen das Netzwerkteam bei der Einrichtung der Firewall und sollen hierzu einige Vorbereitungen treffen.

aa) Erläutern Sie, was eine „Stateful Packet Inspection" Firewall von einem reinen Paketfilter unterscheidet. 4 Punkte

ab) Bislang wurden folgende Internet-Anwendungen identifiziert, welche durch die Firewall ermöglicht werden sollen:
- HTTPS
- SMTP/IMAPS
- Externe Datenbankanwendung, welche auf Port 4711 reagiert
- Interner Webserver muss von außen über eine gesicherte HTTP-Verbindung unter IP 192.0.2.64 erreichbar sein

Allen weiteren Datenverkehr soll die Firewall unterbinden.

Vervollständigen Sie die Regeln für die Stateful Packet Inspection Firewall in folgender Tabelle. 9 Punkte

Regel	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
allow	TCP	any	any	any		out
allow	TCP			any	587 (smtp)	out
allow		any	any		993 (imaps)	out
	TCP	any	any	any	4711	out
allow	TCP	any	192.0.2.64/32	any		in
	any	any	any	any	any	out
	any	any	any	any	any	in

ac) Für die Absicherung des Netzwerks müssen Sie eine moderne Firewall beschaffen. Sie erwägen, eine „Next Generation Firewall" anzuschaffen.

Erläutern Sie zwei Vorteile, die eine solche Firewall im Vergleich zu einem klassischen Paketfilter bietet. 4 Punkte

Korrekturrand

b) Für die geplanten VPN-Tunnel zwischen den Standorten stehen derzeit zwei alternative Software-Produkte zur Auswahl:

VPN-Software 1, welche Zertifikate nach X.509 einsetzt, um beide Seiten der Verbindung gegenseitig zu authentifizieren.

oder

VPN-Software 2, welche zur Authentifizierung eigene Public-Keys generiert, die durch die Administratoren auf den jeweiligen Geräten hinterlegt werden müssen.

ba) Wählen Sie eines der beiden genannten Produkte aus und begründen Sie Ihre Entscheidung. 4 Punkte

bb) Bei der Auswahl der Hardware für die VPN-Tunnel fallen einige Kriterien auf.

Erläutern Sie deren Relevanz in Bezug auf die Funktionalität der Tunnel: 8 Punkte

– hardware-unterstützte Krypto-Algorithmen:

– Anzahl Netzwerkports:

– garantierte Firmware-Updates über einen bestimmten Zeitraum:

– Leistungsaufnahme in Watt:

4. Aufgabe (20 Punkte)

Korrekturrand

Steigende Energiekosten haben die IHK-Wear GmbH dazu veranlasst, Energiedaten für die Räume zu erfassen. Dazu werden neben bereits fest installierten Sensoren nun auch IoT-Geräte eingesetzt, welche die Temperatur und Luftfeuchtigkeit in jedem Raum messen und per Funk übertragen.

a) Die neuen IoT-Geräte werden an das WLAN der Firma angebunden.

aa) Die neue WLAN-SSID für die IoT-Geräte stellt keinen SSID-Broadcast zur Verfügung.

Beschreiben Sie die Funktionsweise und den Zweck des SSID-Broadcasts. 2 Punkte

ab) Damit die IoT-Geräte in das WLAN integriert werden können, müssen die Authentifizierung und die Vertraulichkeit festgelegt werden.

Erläutern Sie die beiden Begriffe in Bezug auf die WLAN-Verbindung. 4 Punkte

Authentifizierung:

Vertraulichkeit:

ac) Nennen Sie jeweils ein Beispiel, wie WPA (1/2/3) die Authentifizierung bzw. Verschlüsselung realisiert. 2 Punkte

Beispiel für Authentifizierung:

Beispiel für Verschlüsselung:

b) Sobald ein IoT-Gerät eine Verbindung zum WLAN hergestellt hat, versucht es, automatisch eine IP-Adresse vom DHCP-Server zu erhalten.

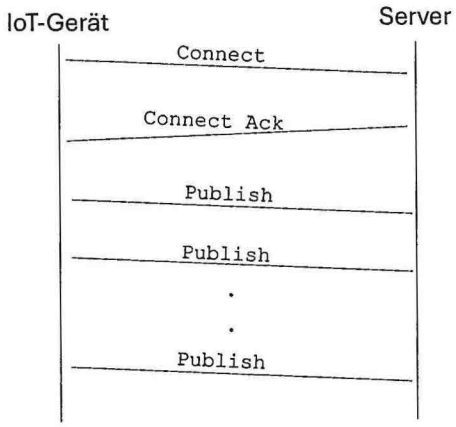
ba) Erläutern Sie, warum der DHCP-Discover als Broadcast erfolgt. 3 Punkte

Korrekturrand

bb) Nachdem der DHCP-Vorgang erfolgreich abgeschlossen ist, sendet das IoT-Gerät (bzw. jeder neue Client) sogenannte „Gratuitous ARP-Requests".

Erläutern Sie den Sinn dieser ARP-Requests. 3 Punkte

c) Die Datenübertragung der IoT-Geräte erfolgt per MQTT. Der Verbindungsablauf zwischen einem exemplarischen IoT-Gerät und dem Server ist nachfolgend abgebildet.



ca) Erläutern Sie, warum das MQTT-Protokoll auf TCP und nicht auf UDP aufsetzen muss. 3 Punkte

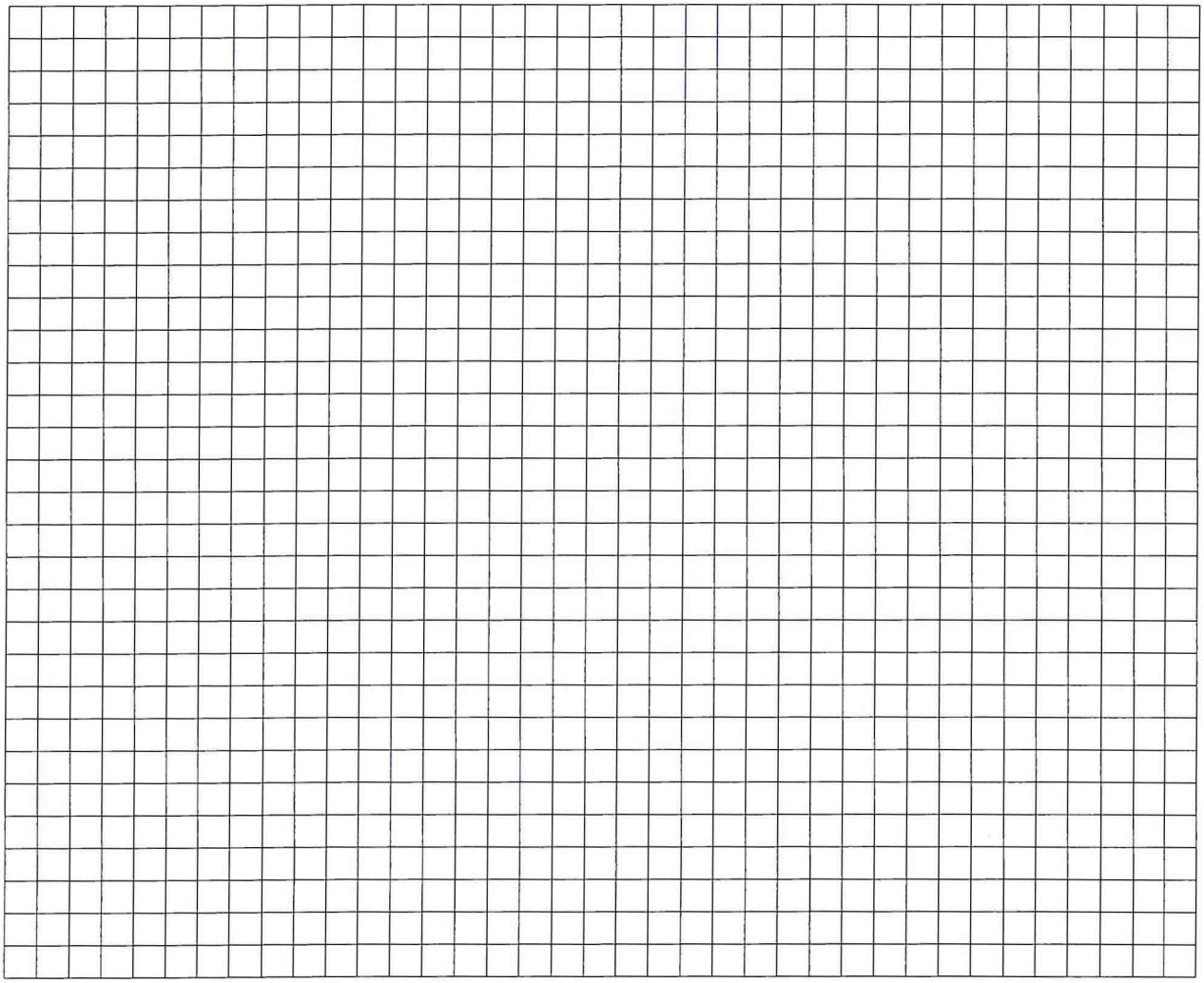
Fortsetzung 4. Aufgabe →

Fortsetzung 4. Aufgabe

Korrekturrand

cb) Eine einzelne „Publish Message" ist 66 Byte groß und wird periodisch alle 60 Sekunden gesendet. Insgesamt senden zukünftig 500 IoT-Geräte ihre Sensordaten per MQTT an den Server.
Die WLAN-Bandbreite für diese SSID soll auf lediglich 10 kbit/s begrenzt werden.

Bestimmen Sie durch Rechnung, ob die gewählte Bandbreite ausreichend ist. Hinweis: Protokolloverhead muss nicht berücksichtigt werden. 3 Punkte



PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

[1] Sie hätte kürzer sein können.
[2] Sie war angemessen.
[3] Sie hätte länger sein müssen.

Abschlussprüfung Sommer 2025
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).
Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=	100 – 92 Punkte	Note 2	= unter	92 – 81 Punkte
Note 3	= unter	81 – 67 Punkte	Note 4	= unter	67 – 50 Punkte
Note 5	= unter	50 – 30 Punkte	Note 6	= unter	30 – 0 Punkte

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2025 – Alle Rechte vorbehalten!

1. Aufgabe (22 Punkte)

aa) 4 Punkte

VLAN ID	Name	Subnetz	Maske	Anzahl Adressen
1	default	192.168.1.0/24	255.255.255.0	254
11	Technik	192.168.11.0/26	255.255.255.192	62
12	Vertrieb	192.168.12.128/25	255.255.255.128	126
66	Management	192.168.66.8/29	255.255.255.248	6
	Fililal-Netze	172.16.200.0/22	255.255.252.0	1022

ab) 4 Punkte

VLAN ID	Name	Subnetz	Gateway
1	Default	192.168.1.0/24	192.168.1.254
11	Technik	192.168.11.0/26	192.168.11.62
12	Vertrieb	192.168.12.128/25	192.168.12.254
66	Management	192.168.66.8/29	192.168.66.14

ac) 4 Punkte

Für jedes VLAN und dem damit verknüpften Subnetz wird ein Gateway benötigt.
Da der Router nur über zwei physikalische Schnittstellen (eth0 und eth1) verfügt, müssen auf der zum LAN führenden Schnittstelle Subinterfaces eingerichtet werden.
Ein Subinterface ist eine virtuelle Schnittstelle, die durch Unterteilen einer physischen Schnittstelle in mehrere logische Schnittstellen erstellt wird.

ba) 4 Punkte

Link aggregation:
Standard zur parallelen Bündelung von mehreren physischen Netzwerkverbindungen zu einer logischen
Erlaubt die Verteilung von Ethernet Frames auf alle verfügbaren physischen Links

Vorteile:
Höhere Verfügbarkeit
Höhere mögliche Übertragungsgeschwindigkeit bzw. höherer Datendurchsatz

bb) 4 Punkte

- Um Schleifen im Netzwerk zu vermeiden.
- Das Spanning Tree Protokoll hat diesen Port geblockt, um Schleifen im Netzwerk zu verhindern.
- Der Admin hat den Port geblockt, um Schleifen zu vermeiden.
- Andere Lösungen sind denkbar.

c) 2 Punkte

Default Route einrichten 0.0.0.0/0 über eth0 oder Next-Hop-IP (203.0.113.2), sodass alle sonst möglichen Adressen über die Schnittstelle eth0 erreicht werden können.

2. Aufgabe (29 Punkte)

aa) 3 Punkte

- Bessere Reaktions- und/oder Bearbeitungszeit zur Fehlerbehebung
- Geschäftskunden-Hotline
- Feste IP-Adresse
- Garantierte Verfügbarkeit
- u. a.

ab) 3 Punkte

- Shared Medium: Bei Gigabit Passive Optical Networks (GPON) wird eine Glasfaser für mehrere Kunden verwendet, diese teilen sich die verfügbare Bandbreite.
- Für die Filiale ungünstig,
  - da evtl. nicht die volle Bandbreite zur Verfügung steht
  - da evtl. keine feste IP-Adresse vorhanden
  - u. a.

ac) 4 Punkte

- LTE funktioniert über das Mobilfunknetz.
- Über LTE bekommt der Kunde nur eine private IP-Adresse für die Internetanbindung (CGN, Carriere Grade NAT).
- Geschwindigkeit im Angebot ist wesentlich geringer als bei den anderen Angeboten.
- Die tatsächliche Geschwindigkeit kann nochmals unterhalb dieser Angabe liegen, da ebenfalls Shared Medium.
- Weitere Gründe sind möglich.

ba) 4 Punkte
- Die Geräte in der Filiale werden mit privaten IPv4-Adressen ausgestattet.
- Der Router, der die Verbindung zum Internet herstellt, übersetzt bei den ausgehenden Datenpaketen mit NAT und PAT die Quell-IP-Adresse und den Quell-Port.
- Die Datenpakete werden mit der öffentlichen IP-Adresse als Absenderadresse ins Internet gesendet. Antworten können so auch wieder an diese öffentliche IP-Adresse zurückgesendet werden.
- Andere Formulierungen sind möglich.

bb) 5 Punkte
- 256 Subnetze
- 1. Subnetz: 2001:db8:9876:: /64
- 2. Subnetz: 2001:db8:9876:0001:: /64
- Vorletztes Subnetz: 2001:db8:9876:00fe:: /64
- Letztes Subnetz: 2001:db8:9876:00ff:: /64

bc) 2 Punkte
- Eine DMZ ist ein separates Netzwerk.
- Eine DMZ wird durch einen oder mehrere Router/Firewall vom eigentlichen LAN getrennt.
- Dort werden Geräte untergebracht, die von außen erreichbar sein sollen, um das eigentliche Netzwerk bei einem Angriff zu schützen.
- Kein direkter Durchgriff auf Geräte im LAN.

bd) 2 Punkte
- In einem /64 Netzwerk existieren 2^{64} IP-Adressen.
- Rund 1,84 x 1.019
- Der exakte Wert (18.446.744.073.709.551.616) muss nicht ausgeschrieben genannt werden, um die Punkte zu erhalten.

ca) 1 Punkt
Der Client sendet die Anfrage komplett an den eingetragenen DNS-Server weiter.

cb) 3 Punkte
Der Router fragt …
- bei den Root-Servern nach den DNS-Servern für den DE-Bereich.
- bei den DE-Servern nach dem DNS-Server für ihk.de.
- bei den Servern von ihk.de nach der IP-Adresse von www.ihk.de.

cc) 2 Punkte
- Wird ein öffentlicher DNS-Server verwendet, so können interne Domain-Namen nicht mehr aufgelöst werden.

oder
- Interne Server wären sonst nur noch über ihre IP-Adresse erreichbar, nicht mehr über ihren DNS-Eintrag.

Ähnliche Antworten sind auch gültig.

3. Aufgabe (29 Punkte)

aa) 4 Punkte
SPI erfasst zugelassene Datenströme (i. d. R. TCP, UDP und ICMP) als sogenannte „States". Wenn auf einen erfassten Datenstrom Antworten erfolgen, werden diese ohne weitere Prüfung zugelassen. Ein reiner Paketfilter erkennt „Antwort-Traffic" nicht automatisch.

ab) 9 Punkte

Regel	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
allow	TCP	any	any	any	443	out
allow	TCP	any	any	any	587	out
allow	TCP	any	any	any	993	out
allow	TCP	any	any	any	4711	out
allow	TCP	any	192.0.2.64/32	any	443	in
reject	any	any	any	any	any	out
deny	any	any	any	any	any	in

Lösungshinweis für Korrektor: reject, deny (oder sinngleiche Ausdrücke) werden austauschbar akzeptiert

ac) 4 Punkte
- Intrusion Detection System/Intrusion Prevention System – automatische Erkennung und Abwehr von externen Angriffen (z. B. Abwehr von SYN Flood)
- Schadsoftwareerkennung – Filterung des Datenverkehrs (z. B. eingehende SMTP, Web, SQL, SMB-Verbindungen)
- Anti-Virus-/Anti-SPAM-Filter Mail-Relay – Filterung von eingehenden E-Mails auf bekannte Schadsoftware/SPAM-Merkmale
- QoS-Management – Priorisierung von Netzwerkdiensten (z. B. VoIP) und Bereitstellung abgestufter Bandbreiten für die Datenübertragung
- Payload des Datenstroms – Anwendungen werden identifiziert und können blockiert oder in der Nutzung der Bandbreite eingeschränkt werden.
- u. a.

ba) 4 Punkte
VPN-Software 1: Zertifikate sichern die Public-Keys mithilfe einer CA durch Signaturen ab. Aber eine CA ist notwendig.

VPN-Software 2: benötigt keine CA (weder intern noch extern), dadurch weniger administrativer Aufwand. Aber höhere Disziplin seitens der Admins gefordert.

bb) 8 Punkte
- Hardware-unterstützte Krypto-Algorithmen

Hohe Relevanz, da ein deutlicher Perfomance-Verlust zu erwarten ist, wenn die Algorithmen der SW nicht unterstützt werden

- Anzahl Netzwerkports

Muss ausreichend sein für die Anzahl der physikalischen Verbindungen (ggf Link-Aggregation)

- Garantierte Firmware-Updates über einen bestimmten Zeitraum

Ohne Firmwareupdates ist kein Einsatz im sicherheitsrelevanten Umfeld sinnvoll.

- Leistungsaufnahme in Watt

Keine Auswirkung auf die VPN-Tunnel.

4. Aufgabe (20 Punkte)

aa) 2 Punkte
Durch SSID-Broadcast sendet das drahtlose Netzwerk regelmäßig seine SSID aus, damit WLAN-Geräte diese sehen können, um sich damit zu verbinden.

ab) 4 Punkte
Authentifizierung:
Bei der Authentifizierung wird die Identität eines Benutzers oder auch Geräts überprüft, um sicherzustellen, dass sie berechtigt sind, auf das Netzwerk zuzugreifen.

Vertraulichkeit:
Durch die Vertraulichkeit sollen die Daten, die per Funk übertragen werden, vor Unbefugten geschützt werden.

Andere Formulierungen sind möglich.

ac) 2 Punkte
Beispiel für Authentifizierung: festes PW mit z. B. PSK, individuelle Zugangsdaten durch z. B. RADIUS, Zertifikat

Beispiel für Verschlüsselung: AES, TKIP

Andere Lösungen sind möglich.

ba) 3 Punkte
Der DHCP-Discover wird an alle Geräte im lokalen Netzwerk gesendet, da der Client selbst noch keine IP-Adresse besitzt und ihm auch die Adressen des DHCP-Servers bisher noch nicht bekannt sind.

bb) 3 Punkte
Client findet so heraus, ob die vom DHCP-Server vergebene IP-Adresse tatsächlich frei ist.

ca) 3 Punkte
Da die Daten an einen bestimmten Server (MQTT-Broker) gesendet werden, muss ein Verbindungsaufbau stattfinden, der die Zuverlässigkeit der Publish Messages sicherstellt.

cb) 3 Punkte (2 Punkte Berechnung, 1 Punkt Schlussfolgerung)
Beispielrechnung:
Datenverbrauch alle Geräte
66 Byte * 500 (Geräte) = 33.000 Byte

Datenverbrauch pro Sekunde
33.000 Byte / 60 Sekunden = 550 Byte/s

Benötigte Bandbreite für alle 500 Geräte pro Sekunde in kbit/s:
550 Byte/Sekunde * 8 bit/Byte = 4.400 bit/s = 4,4 kbit/s

Da nur 4,4 kbit/s benötigt werden, ist die gewählte Bandbreite von 10 kbit/s ausreichend.